REMARKS

Applicants respectfully traverse and request reconsideration.

Applicants wish to thank the Examiner for the withdrawal of the 35 U.S.C. §101 rejections as to certain claims. Claims 18-19 and 24-27 however still stand rejected under 35 U.S.C. §101 as allegedly being directed to non-statutory subject matter. As to claim 18, it claims "a network element comprising" and is in "means plus function format" but is nonetheless alleged to "refer to a software network element comprising software means." Applicants respectfully challenge this assertion as Applicants are uncertain as to what "software means" refers to. In addition, the office action misstates the wording of a cited portion of the Specification, namely pages 7-8. For example, it is alleged that the Specification defines a network element such that it "may be an intranet" (see office action, page 6). However, this is a misstatement of the application. The application states:

> The network element 16A may be implemented as a server suitably coupled to one or more wide area networks or local area networks as desired.

As such, the language is clear that the network element may be implemented as a server and that the server may be coupled to one or more wide area networks or the server may be coupled to a local area network. It does not say that a server may be an intranet. In fact, the portions on pages 7 and 8 (see paragraph 19) actually states the network element includes a transceiver 22, a decryptor and an encryptor and that the encryptor includes one or more processing devices that may execute instructions to cause the processing devices to carry out the operations described herein or alternatively that the network element may include discrete logic or any suitable combination of hardware, software and firmware. This defines structure and is but one embodiment. Applicants respectfully submit that the claim is compliant with section 101 as written.

Claim 19 is also in proper form for the reasons stated above.

Claim 24 also is alleged to not comply with 35 U.S.C. §101. Again, Applicants are confused as to the rejection as it merely states "Claim 24 recites a secure communication system which can be implemented in software alone as a limitations it comprises all read on software elements". This is inconsistent with the Specification and there is no factual support for such statement. If the rejection is maintained, Applicants respectfully request a showing as to where the Specification states that a "secure communication system" is merely software per se. For example, claim 24 requires a network element, a sender, and an intended recipient and also includes means plus function language which by its definition includes structure. Accordingly, Applicants respectfully submit that the claim is in proper form.

Claims 1, 3-8, 10, 15, 17-20, 22-24 and 26 stand rejected under 35 U.S.C. §102(e) as being anticipated by Pearlman. The rejection includes new cited portions of this reference and also apparently attempt to combine structures within Pearlman to read on Applicants' claimed network element. As a preliminary matter, Applicants respectfully disagree that the previous amendment with respect to claim 1 changes the scope of the claim as the claim originally existed, it indicated that the method includes receiving both encrypted information from a sender for transmission to at least one intended recipient and receiving an encrypted secret key encrypted using a public key associated with a secure distribution server. The amendment was made merely for clarification purposes as it appeared that the Examiner may have been misapprehending the claim in view of the Specification and as understood by one of ordinary skill in the art.

On page 5 of the rejection, the office action states that the Examiner is combining the functions of the distribution list exploder (DLE) and group server into just the DLE. Such a combination still does not anticipate Applicants' claimed invention. As Applicants previously noted, Pearlman is directed to a method and apparatus for sending encrypted electronic mail through a distribution list exploder which forwards an encrypted message to a

recipient in a distribution list but utilizes a group public key of a group server to form an encrypted message key. As such, Pearlman requires the use of a group server namely certificate server 116. "The group public key is associated with a group private key to form a public key-private key pair associated with a group of valid recipients for the message." (See Abstract and other sections of Pearlman). The system of Pearlman is distinct from Applicants' claimed invention.

For example, as to claim 1, the method requires among other things, receiving an encrypted secret key encrypted using a public key associated with a secure distribution server. The method also includes decrypting the encrypted secret key to produce a decrypted secret key and encrypting the decrypted secret key for at least one intended recipient using a corresponding public key to produce at least one recipient specific secure secret key.

The office action cites, for example, column 7, lines 41-59 as allegedly teaching obtaining a corresponding public key of at least one intended recipient and encrypting the decrypted key using the corresponding public key to produce a recipient specific secure secret key. However, the cited portion does not teach such an operation. To the contrary, the cited portion refers to FIG. 4C wherein a group server decrypts the encrypted message key and "then encrypts the message key with group secret key 314" (emphasis added). As such, this teaches re-encrypting a decrypted secret key using a group secret key. This does not teach encrypting the secret key using a public key of a recipient to produce at least one recipient specific secure secret key as required by the claim. A key encrypted using a group key can be decrypted by groups of recipients that share a common public key. In contrast, Applicants claim a "recipient specific" encryption technique in combination with other limitations so that multiple recipients cannot use the same public key to decrypt the secret key unlike the system taught in the cited portion of Pearlman. Accordingly, the claim is in

condition for allowance for this reason alone. One of ordinary skill in the art will recognize other distinctions as well.

Applicants respectfully reassert the relevant remarks made above with respect to the other independent claims and as such, these claims are also in condition for allowance.

The dependent claims add additional novel and non-obvious subject matter. As such, these claims are also in condition for allowance.

Claims 2, 9, 12-13, 16, 21 and 25-26 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Pearlman. Applicants respectfully reassert the relevant remarks made above with respect to Pearlman and as such, these claims are also in condition for allowance.

Claims 11 and 27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Pearlman in view of Chen. Applicants respectfully reassert the relevant remarks made above with respect to Pearlman and as such, these claims are also in condition for allowance.

Claim 14 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Pearlman in view of Bouchard et al. Applicants respectfully reassert the relevant remarks made above with respect to Pearlman and as such, this claim is also in condition for allowance. This claim also adds additional novel and non-obvious subject matter.

Applicants respectfully request that a timely Notice of Allowance be issued in this case. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

Date: 7/19/06

By: _____
Christopher J. Reckamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz, P.C.
222 N. LaSalle Street
Chicago, Illinois 60601
PHONE: (312) 609-7599
FAX: (312) 609-5005